

REMARKS

I. Introduction

In response to the Office Action dated September 11, 2003, claims 1, 2, 18, 25, and 26 have been amended. Claims 1-37 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. Office Action Objections

In paragraph (1), the Office Action objects to the drawings as failing to comply with 37 C.F.R. 1.84(p)(5) because they include reference signs not mentioned in the description. With respect to reference signs 116, and 212, and 526, the Applicants have amended the specification to call out these reference signs and to correct errors. Reference sign 420, is included in the specification at page 19, line 25. Therefore, no further amendment is required.

IV. Enablement Rejections

In paragraph (4), the Office Action rejects claims 16-24 under 35 U.S.C. § 112, first paragraph, for failing to comply with the enablement requirement. According to the Office Action, the claims contain subject matter that was not described in the specification in such a way as to enable one of ordinary skill in the art to make or use the invention. The Office Action indicates that claim 16 claims a fourth decryption module, and that a fourth decryption module is not disclosed in the specification or the drawings. The Applicants respectfully traverse these rejections, as the features described in claim 16-24 are disclosed in both the drawings and the text of the Applicants' specification as described below.

With Respect to Claim 16: Claim 16 describes an embodiment in which the media program (which is encrypted by the CW key when received) is further encrypted before storage. When this media program is later played back, it is decrypted (returning it into a form analogous to that which was initially received), then decrypted using the CW extraction module in the CAM 406, and the broadcast decrypt module 510. This embodiment is described in the Applicants' specification from page 13 line 26 to page 19, line 4 of the Applicants' specification, and is illustrated in FIGs. 5A and 5B. Specifically, the features described in claim 16 are disclosed in the specification as follows: a first encryption module (512), a second encryption module (522), a first decryption module (532), a second decryption module (534), a conditional access module (406) having a third decryption module (544) for decrypting encrypted access control information to produce the CW key, and a fourth decryption module (510) for decrypting the encrypted program material using the CW key.

With Respect to Claim 17: The Office Action rejects claim 17 because the Examiner could not find any support for the second media storage device, third encryption module, or the fourth and fifth decryption module in the specification and the drawings.

Claim 17 describes a further refinement of the embodiment described in claim 16. As described in the Applicants' specification from page 19, line 5 to page 21, line 9, and illustrated in FIG. 5C, this embodiment supports "trick play" functionality such as rewinding and fast forwarding through the media program. In this embodiment, a third encryption module (550) is used to re-encrypt the media program that was decrypted by the fourth decryption module (510), and a fifth decryption module (554) is used to decrypt the program material encrypted by the third encryption module (550). The second storage device is described in the Applicants' specification as follows:

In this embodiment, the unencrypted program material 511 is not provided directly for display, but rather copy protection encrypted, stored in the data storage device 528 (or a second data storage device), and retrieved and decrypted before providing the program material for display. In particular, the unencrypted program material 511 is provided to a second Storage Encrypt Module 550. The second Storage Encrypt Module 550 encrypts the unencrypted program material 511 using the CP encryption key 516 to produce re-encrypted program material 552. The CP encryption key 516 is also encrypted by the key encrypt module 522 to produce the encrypted CP key 524. Both the re-encrypted program material 552 and the encrypted CP key 524 are stored in the media storage device 528, as shown in block 558. (Specification, page 19 lines 15-24, emphasis added).

and

Finally, it is noted that in the embodiment described above, the media storage device 528 depicted in FIG. 5C is the same media storage device 528 depicted in FIG. 5A. If desired, however, the re-encrypted program material 552 can be stored in a second (and separate) media storage device. For that matter, any of data described in the foregoing can be stored in a plurality of media storage devices to increase throughput or facilitate additional security measures. This embodiment would permit faster storage and retrieval of information from the disk(s). (Specification, page 20 line 29 through page 21 line 4).

Given the foregoing, the Applicants believe that claims 16-24 comply with 35 U.S.C. § 112.

V. The Cited References and the Subject Invention

A. The Lee Reference

U.S. Patent No. 6,266,481, issued July 24, 2001 to Lee et al. (Lee) discloses a conditional access system for a local storage device. Lee discloses a technique for selectively inhibiting a video recorder from recording and/or reproducing those television programs, which are not authorized for viewing. Authorization data associated with respective television programs that are receivable by the recorder and indication of whether that program is authorized for recording and/or reproduction, is received by the recorder prior to (or multiplexed with) the television program and is stored thereat. When the television program is received, the stored authorization data associated with that is read to determine if the received television program is authorized for recording and/or reproduction. If not, the recorder is inhibited from recording and/or reproducing that unauthorized television program.

B. The Park Reference

U.S. Patent No. 5,761,302, issued June 2, 1998 to Park (Park) discloses a copy prevention method and apparatus for a digital video system. The method includes the steps of: (a) adding a header area of a header start code and key field to a reproduced bit stream; (b) decrypting and transmitting the bit stream to which the header area is added; (c) detecting a key field of the decrypted and transmitted bit stream and detecting copy prevention information; and (d) encrypting the bit stream according to information detected from step (c) and recording it on tape.

VI. Office Action Prior Art Rejections

In paragraph 6, the Office Action rejected claims 1-16 and 20-37 under 35 U.S.C. § 103(a) as unpatentable over Lee in view of Park. The Applicants respectfully traverse these rejections.

With Respect to Claim 1: At the outset, it is important to understand what Lee teaches and what it does not. Lee teaches a system which prevents the user from recording program received on a particular channel without authorization.

In one embodiment (FIGs. 2 and 3), this is accomplished by using a conditional access module 13 to control the playback and recording of data. The conditional access module 13 reads authorization data, and disables the operation of the digital VCR and/or causes a visual indication to be displayed to the subscriber. If the subscriber wants to record the program, they are to contact the authorization center (see col. 5, lines 47-60).

If subscriber is authorized to record the program, the program is descrambled and recorded on the VCR. (col. 6, lines 21-30). Also, authorization data is stored on the tape indicating whether the subscriber has the right to *reproduce* the program. When the recorded videotape is played, the conditional access module 13 reads the smartcard and the data recorded on the tape for reproduction rights. If reproduction is not permitted, it indicates as such to the user. If reproduction is authorized, it is provided through appropriate circuitry for viewing.

In another embodiment (FIG. 3), the program data is encrypted by keys K_s (and optionally K_w) before being sent to the subscriber, and the conditional access module 13 reads the authorization data from the smartcard, and if the subscriber is authorized to record the program, the program is descrambled and supplied to the VCR for recording. (col. 8, lines 38-50). Since it is risky to send keys K_s or K_w plaintext, they can be encrypted by a unique personal key K_p before transmission.

Lee teaches that if it is not desirable to leave an unencrypted version of the program in storage or to expose it to "tapping" while recording, the program should be encrypted at the headend with a modification key K_m before being encrypted with key K_s (see col. 10, lines 9-24). K_s is still used to descramble the program, but the program remains encrypted by the modification key K_m when it is stored in local storage 45. In

essence, the program is doubly encrypted at its source and only singly decrypted before storage to keep subscribers who do not have viewing privileges from viewing the program while it is recorded and to prevent subscribers without reproduction privileges from reproducing it.

As described in claim 1, the Applicants' invention receives encrypted program material and encrypted control information at the subscriber, and *further* encrypts both the *received* encrypted program material and the *received* encrypted access control information according to a second encryption key (e.g. the copy protection key) before storage.

Lee teaches storing generating doubly encrypted program material at the head end, and protecting the program material from unauthorized viewing or reproduction by storing a singly decrypted version of the material at the subscriber. Lee does not recognize the problem that storing a singly encrypted version of the program material exposes the program material and the information used to decrypt it to compromise. This is especially a problem for encryption schemes that are non-stationary, or time varying, because the ability to store and replay this information permits hackers. As described in the Applicants' specification:

An I/O indecipherable algorithm is an algorithm that is applied to an input data stream to produce an output data stream. Although the input data stream uniquely determines the output data stream, the algorithm selected is such that it's characteristics cannot be deciphered from a comparison of even a large number of input and output data streams. The security of this algorithm can be further increased by adding additional functional elements which are non-stationary (that is, they change as a function of time). When such an algorithm is provided with identical input streams, the output stream provided at a given point in time may be different than the output stream provided at another time.

So long as the encryption module 218 and the IRD 132 share the same I/O indecipherable algorithm, the IRD 132 can decode the information in the CWP to retrieve the CW. Then, using the CW, the IRD 132 can decrypt the media program so that it can be presented to the subscriber 110.

To further discourage piracy, the control data needed to decrypt and assemble data packets into viewable media programs may be time-varying (the validity of the control data in a CWP to decode a particular media program changes with time). This can be implemented in a variety of ways.

For example, since each CWP is associated with a SCID for each media program, the SCID related to each CWP could change over time.

Another way to implement time-varying control data is to associate time stamps with the received data stream and the CWP control data. In this case, successful decoding of the CWP to produce the CW would require the proper relationship between the time stamps for the data stream and the control data in the CWP. This relationship can be defined, for example, by changing the decryption scheme used to generate the CW from the CWP according to the received time stamp for the data stream. In this case, if the time stamp of the received data stream does not match the expected value, the wrong decryption scheme will be selected and the proper CW (to decrypt the

program material) will not be produced. If, however, the time stamp of the received data stream matches the expected value, the proper decryption scheme will be selected, and the CWP decryption scheme will yield the proper CW. (Specification, page 10, line 7 through page 11, col. 5).

Because Lee stores program material singly encrypted by key K_m , it potentially exposes the recorded program to hacking. As described in the Applicants' specification:

While it would presumably be possible to simply store the datastream as it is received from the broadcaster for later replay, this technique has distinct disadvantages. One such disadvantage is that it would provide pirates a permanently recorded version of the encrypted datastream, thus providing the pirate with information that can be used to perform detailed analyses of the datastream itself to determine the encryption techniques and codes. (Specification, page 3, lines 7-12)

The Applicants' invention prevents this problem by *further* encrypting both the encrypted program itself, and the encrypted key used to decrypt the program. As a result, the scheme used to transmit the encrypted program material remains secure.

For this reason alone, the system and method taught in Lee is not analogous to encrypting the received encrypted program material and the encrypted control information before storage.

Further, one of the further advantages of the Applicants' invention is that it does not require any changes to existing equipment (the conditional access module that decrypts the encrypted access control information to produce the first encryption key and the first encryption key). The same cannot be said for Lee, even when combined with the Park reference.

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicant. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994). Because Lee teaches that the program material can be adequately protected with single encryption (and presumably by encryption with larger keys if desired to

prevent hacking), Lee teaches away from the Applicants' invention, and away from any combination with Park.

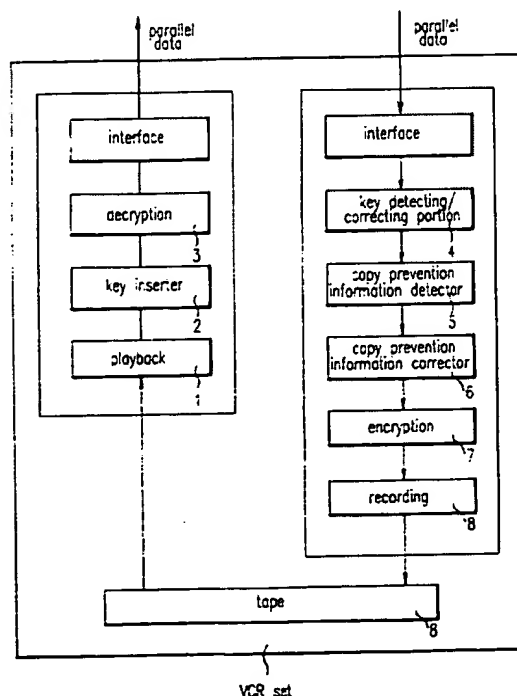
The only remaining issue is whether the Park reference teaches further encryption of the encrypted access control information and the encrypted program material, and whether there is a teaching to modify Lee as disclosed in Park.

Turning to the issue of whether there is a teaching to combine the references, the program should be protected during storage by double encryption at the head end, and storage in a single encrypted form, it is clear that Lee teaches away from the Applicants' invention. The Park reference (including the portions cited in the Office Action, which are reproduced below) does nothing to teach one skilled in the art to do otherwise. The Office Action relies on the following portions of the Park reference:

Therefor, it is an object of the present invention to an illegal copy prevention method and apparatus for a digital video system in which, in copy tape, encrypted key information is transmitted and recorded so that a copied tape is reproducible only in a VCR having a corresponding encrypted key information, thereby preventing copy. (col. 2, lines 40-45)

and

F I G.5



Handwritten mark resembling a heart or a stylized 'B'.

For the foregoing reasons, the Applicants respectfully traverse the rejection of claim 1.

With Respect to Claim 2: Claim 2 recites the decryption of the further encrypted access control material and further encrypted program material. Since the combined Lee and Park references do not teach further encryption, they cannot teach decrypting further encrypted data.

With Respect to Claim 3: Claim 3 recites that the access control information comprises data describing a right associated with the program material. According to the Office Action, this is disclosed as follows:

In addition to the foregoing information included in the program information data, it is a feature of the present invention also to include authorization data stored in the memory of the television receiving apparatus indicating whether a television receiving apparatus is authorized to record and/or reproduce that television program. For example, the authorization data may include authorization status information indicating whether the television receiving apparatus has a limited or complete authorization to reproduce a particular program. The authorization data may further include expiration date data which represents the last date the television receiving apparatus with the limited authorization is authorized to reproduce that program, and price data representing the additional payment required to change the limited authorization status of the television receiving apparatus to the complete authorization status. (col. 4, lines 15-30)

Claim 3 also recites that the step of decrypting the encrypted access control information is performed according to the data describing the right. The Office Action indicates that this is disclosed as follows:

When scrambled signals constituting a program are supplied to the television receiving apparatus, the conditional access circuit determines if those signals constitute a program that is authorized for recording by the television receiving apparatus. If the conditional access circuit determines that the television receiving apparatus is authorized to record that program, a decryption unit 38 of the conditional access circuit 13 decodes the received working key Kw with the pre-stored personal key Kp using conventional decoding (decryption) techniques and supplies the decoded working key Kw to the decryption unit 39 of the conditional access circuit 13. (col. 9, lines 49-60)

However, as far as the Applicants can ascertain, nothing in Lee discloses access control information being encrypted and stored. Instead, access control information (termed "authorization data" in the Lee reference) appears to be simply requested and stored in the memory of the television screening apparatus (see col. 4, lines 15-30). Accordingly, the Applicants respectfully traverse the rejection of claim 3.



With Respect to Claims 4-9: According to the Office Action, Park discloses that access control information may be multiplexed and transmitted on the same channel as the video programming (the Applicants cannot ascertain where this is disclosed in Park -- FIG. 2, for example, discloses an unencrypted datastream). According to the Office Action, this reads on expressing program material rights in the form of a metadata table, but the Applicants respectfully disagree. Even if the Office Action's statements regarding the Park reference were true, simply multiplexing access control information does not fairly disclose expressing rights in a metadata table.

Claim 5-9 recites even more features that are not disclosed or taught by Lee or Park. Nothing in either reference fairly discloses pre-cacheing program material, metadata tables or default values.

With Respect to Claims 10-15: Claim 10 recites features relating to trick play. In the Applicants' invention, such features are supported without storing the program material in unencrypted form. Accordingly, claim 10 recites that the program material that was further encrypted, and decrypted twice (first to decrypt "further" decryption, and second to decrypt the result to obtain the original signal) is re encrypted by the second encryption key, and stored along with a fourth encryption key generated from the second encryption key.

According to the Office Action, Lee discloses decrypting the program data and control information in order to display it to the user, and Park discloses storing the data in encrypted form. However, Lee teaches that trick play functions should be performed with program material that is stored without encryption (see FIG. 2), and does not teach re-recording anything. Park teaches limiting the right to copy by data stored on the tape itself. Even when combined, Lee and Park fail to teach the Applicants' invention. Claims 11-15 are patentable on the same basis. Accordingly, the Applicants respectfully traverse these rejections.

With Respect to Claims 16 and 20-24: Claim 16 is patentable for reasons analogous to those presented with respect to claim 1. According to the Office Action, Lee discloses a tuner (20) and a first encryption module (41) communicatively coupled to the tuner (20), the first encryption module (41) for further encrypting the encrypted program material and access control information according to a second encryption key (K_m).

However, this is incorrect. The “scrambler” 42 of Lee does not “further encrypt the encrypted program material”, because the input to the scrambler 41 is unencrypted. Further, the scrambler 41 does not encrypt the access control information according to K_m . Instead, (1) a *different* encryptor 42 accomplishes that task, and (2) that task is accomplished by a *different* key (K_p).

The Office Action also indicates that the Lee reference discloses a second encryption module (30) communicatively coupled to the first encryption module (41) for encrypting the second encryption key (K_m) according to a third encryption key (K_w) to produce a fourth encryption key (which the Office Action does not identify). This too is incorrect. The scrambler (30), while it may be communicatively coupled to scrambler (41), it does not encrypt “second key” (K_m).

The Office Action further indicates that Lee discloses a first and second decryption module. The Office Action indicates that the second decryption module is descrambler (44), but does not point out where the first decryption module may be found. Claim 1 recites that the first decryption module is communicatively coupleable to a disk drive and decrypts the fourth encryption key to produce the second encryption key. Lee and Park disclose no such structure.

Numerous other structural features recited in claim 16 (as well as claims 20-24) are not disclosed in the Lee reference, nor does the Park reference cure these deficiencies. Accordingly, the Applicants respectfully traverse the rejection of claims 16 and 20-24.

With Respect to Claims 25-37: Claims 25-37 recite features analogous to those of claims 1-15, and are patentable for the same reasons.

With Respect to Claims 17-19: The Office Action’s rejection of claims 17-19 is apparently based solely on the § 112 rejection discussed above. In the event that this was an error, the Applicants’ point out that claims 17-19 recite the features of claim 16 and are patentable on the same basis. Claims 17 and 19 also include limitations that are not cited in the combined Lee and Park references.

VII. Dependent Claims

Dependent claims 2-15, 17-24, and 26-37 recite the features of related independent claims, and are therefore patentable on this basis. In addition, these claims



recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VIII. Conclusion

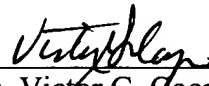
In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: December 11, 2003

By: 
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/io/sjm

G&C 109.40-US-01



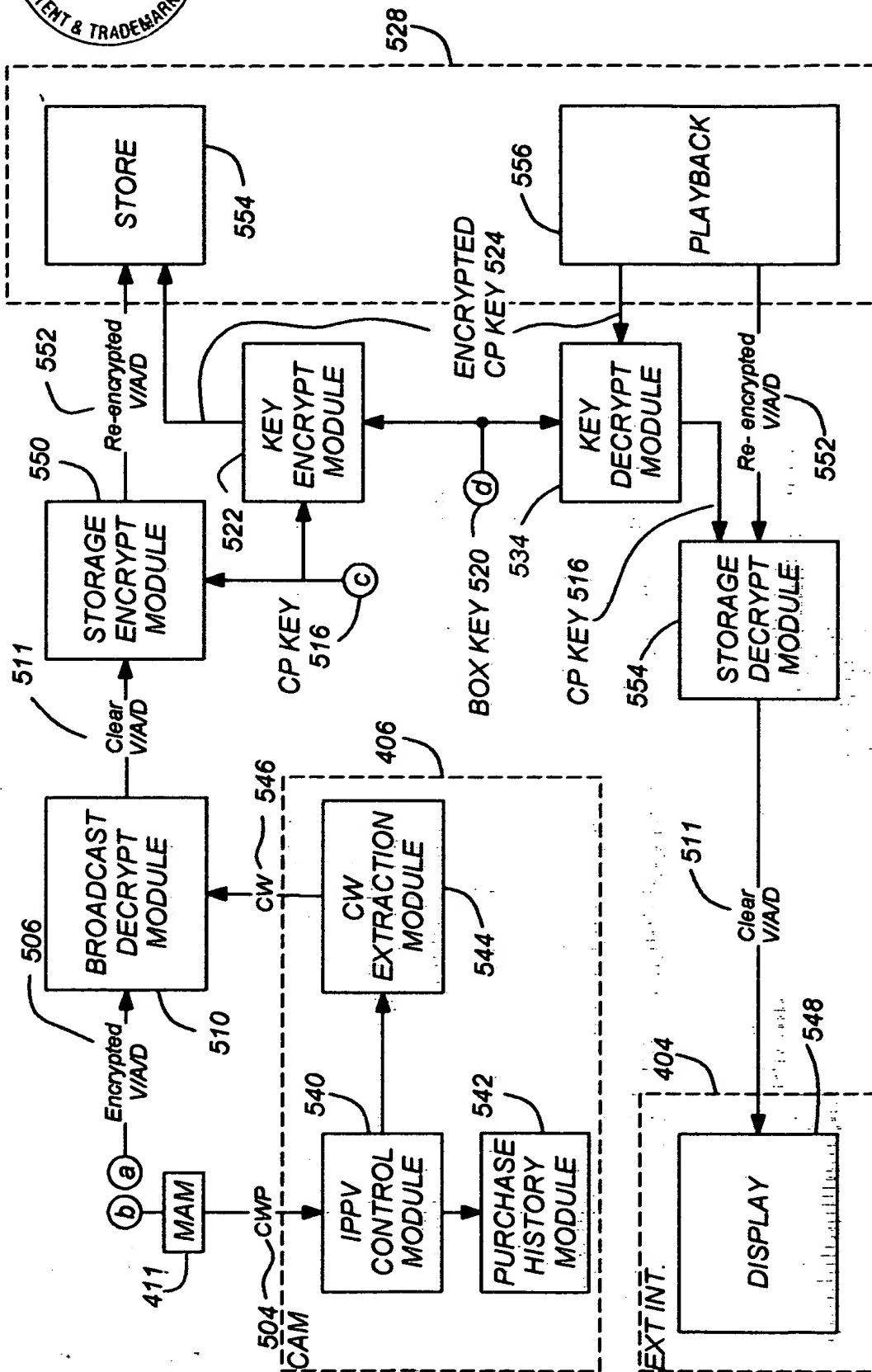


FIG. 5C